CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM

Management Comments and Recommendations

For the Year Ended June 30, 2007

November 13, 2007

To the Finance Committee of the
California Public Employees' Retirement System
Sacramento, California

In planning and performing our audit of the financial statements of the California Public Employees' Retirement System as of and for the year ended June 30, 2007, in accordance with auditing standards generally accepted in the United States of America, we considered CalPERS' internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of CalPERS' internal control. Accordingly, we do not express an opinion on the effectiveness of CalPERS' internal control.

However, during our audit we became aware of several matters that are opportunities for strengthening internal controls and operating efficiency. The memorandum that accompanies this letter summarizes our comments and suggestions regarding those matters. This letter does not affect our report dated November 13, 2007, on the financial statements of CalPERS.

We will review the status of these comments during our next audit engagement. We have already discussed these comments and suggestions with various CalPERS personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

Certified Public Accountants

Sacramento, California
November 13, 2007

INVESTMENT ACCOUNTING

Real Estate Accounting and Reporting

Investment Office, Performance Monitoring Unit

Observation #1. Real estate investment values are derived from independent appraisals when called for by Policy and real estate partnership financial statements. Based on our testing of real estate appraisals, internal controls are not sufficient to ensure that appraised values of real estate investments covered by the CalPERS Investment Policy for Equity Real Estate Appraisal and Valuation are properly recorded by the related partnership. CalPERS established a Performance Monitoring Unit (PMU) in the Investment Office's Administrative Services and Operations Unit. The PMU's responsibility includes selecting appropriate appraisers and finalizing the valuations with the related partnerships, but does not include verifying that appraised values are properly incorporated in the partnership financial records.

We recommend that management implement procedures to ensure that appraised values are properly recorded by the related partnership which should include correlation of appraised property to the partnership financial statements.

Management Response:

Management agrees with the recommendation to implement procedures to ensure that those real estate assets that are appraised subject to Policy, are properly recorded by the related partnership.

Fiscal Services Division, Investment Accounting Unit

Observation #2. We also noted that real estate investment records utilized by the Performance Monitoring Unit (PMU) do not directly correlate with data maintained by Fiscal Services Division's Real Estate Investment Accounting Unit, which increases the risk of errors in the financial reporting process.

We recommend that Fiscal Services Division reconcile quarterly its records in the General Ledger accounts with the records maintained by the PMU of the Investment Office.

Management Response:

Fiscal Services concurs with the recommendation. The Real Estate Investment Accounting Unit has modified the General Ledger Posting Templates used to post partnership financial activity. The General Ledger Posting Templates will include a quarterly reconciliation which will then be compared with the PMU data. Differences, if any, will be investigated and the appropriate adjustments to the General Ledger or PMU reports will be made.

Real Estate Contributions and Distributions Accounts

Observation #3. Real estate contribution and distribution accounts capture cash flow transactions relating to real estate investments. Balances in these clearing accounts typically represent timing differences between State Street Bank records and real estate partnership financial statements. During the fiscal year ended June 30, 2007, Fiscal Services had not sufficiently reconciled the balances. As a result, CalPERS recorded an audit reclassification of approximately $628 million to correct the resulting overstatement of real estate income and expenses.

We recommend that current accounting practices should be evaluated to ensure that real estate contribution and distribution accounts are sufficiently analyzed and related transactions and balances are properly recorded as part of the ongoing accounting function.

Management Response:

Fiscal Services concurs with the recommendation. As part of the Accounting Action Plan 2007 efforts, Fiscal Services is now reconciling the real estate contribution and distribution control accounts on a monthly basis. The reconciling items are identified by partner and will be sufficiently analyzed and recorded.

Real Estate Insurance Premiums

Observation #4. To obtain the most favorable insurance rates, CalPERS purchases property insurance for all real estate investments. The partnership holding the real estate investment is required to reimburse CalPERS for insurance premium payments. During the fiscal year ending June 30, 2007, insurance premiums paid by CalPERS were not tracked and monitored to ensure the respective partnerships properly reimbursed CalPERS. In addition, we noted several partnerships submitted reimbursements directly to Real Estate Investment Accounting rather than the CalPERS Cashier Unit as required by CalPERS policy.

We recommend that management implement procedures to track and monitor the reimbursement of real estate insurance premiums. Outstanding reimbursements should immediately be requested from the respective partnership and payments should be directed to the Cashier Unit.

Observation #4 (Continued)

Management Response:

Fiscal Services concurs with the recommendation. Real Estate Investment Accounting (REIA) will post all payments received for insurance premiums as a reimbursement to CalPERS from the partnership holding the real estate investment. REIA will track and monitor the reimbursement of real estate insurance premiums. REIA will work with the insurance contractor to clear any outstanding receivables due from the partners.

Payments from partnerships will be directed to the Cashiers Unit within Fiscal Services.

Alternative Investments Accounting and Reporting

Observation #5. Alternative investment values are derived from the related partnership's financial statements as reported by PrivateEdge. During our testing, we noted two instances in which the fair values of alternative investments totaling approximately $80 million had been excluded from the year-end PrivateEdge report and the CalPERS general ledger. CalPERS staff did not discover the errors because the investment values reported by PrivateEdge were not reconciled to the underlying partnership financial statements.

We recommend that management implement procedures to ensure that alternative investments are properly valued and reported. Procedures should include reconciling PrivateEdge balances to partnership financial statements as well as evaluating the reasonableness of final valuation adjustments reflected in partnership financial statements.

Management Response:

Fiscal Services concurs with the recommendation. CalPERS will obtain all of the necessary financial statements and reports from the Alternative Investment Partners, and will create a tracking system in order to monitor the receipt of all of the AIM partners reports. Fiscal Services will work with the Investment Office to obtain the financial statements from our partners as promptly as reasonably possible. Upon receipt of the partnerships financial statements, Fiscal Services will evaluate the reasonableness of the balances reported by Private Edge with the partnership financial statements prior to updating the general ledger accounts for year end reporting. Fiscal Services will monitor, evaluate, review, and reconcile the activity and balances of the partner's financial statements based on the quarterly activity, yearly activity and/or prior year activity to ensure that alternative investments are properly valued and reported. Fiscal Services will ensure all partnerships have had the appropriate fiscal year end accruals posted in our financial statements.

Accounting for Unitization Activities

Observation #6. CalPERS has elected to unitize certain investment portfolios in order to commingle the investments of the various plans. During our audit we noted several discrepancies between CalPERS' general ledger investment balances and amounts reflected in State Street Bank records. We determined that several transactions relating to the unitization of investment portfolios were erroneously posted to the general ledger, which resulted in two audit adjustments. We also noted inconsistencies in the way in which unitized and non-unitized portfolios are reported in the financial statements.

We recommend that current accounting practices be evaluated to ensure that investment activities are consistently and accurately reflected in CalPERS' financial records.

Management Response:

Fiscal Services concurs with the recommendation. A cross-functional project team will be established to focus on the improvement of the accounting practices for the unitization of investment portfolios. The team will review the accounting processes performed by the custodian, State Street Bank. The team will also review all associated journal entries posted in PeopleSoft and analyze the impact that it has on the financial statements. The deliverables of this project are to establish standard, repeatable, auditable and meaningful processes for the reconciliation of unitized portfolios and a consistent reporting methodology in the financial statements.

RECONCILATION OF NON-INVESTMENT ACCOUNTS

Reconciliation of Benefit Payments

Observation #7. Retirement benefits are processed in the Retirement Information and Benefits System (RIBS) and the Contribution Reporting System (CRS) subsidiary ledgers, and payments are disbursed by the California State Controller's Office. Fiscal Services reconciles benefit payments recorded in the CalPERS general ledger to the State Controller's Office claims schedule on a monthly basis. However, benefit payments recorded in the general ledger are not periodically reconciled to the underlying RIBS and CRS systems, which is necessary to ensure benefit payments are properly recorded as to period, amount, fund and classification.

We recommend that management implement procedures to reconcile benefit payments recorded in the general ledger to amounts reported in the respective subsidiary ledgers.

Observation #7 (Continued)

Management Response:

Fiscal Services concurs with the recommendation. Fiscal Services will implement procedures to reconcile benefit payments recorded in the general ledger to the Retirement Information and Benefits System (RIBS). Fiscal Services currently reconciles all benefit payments including payments from RIBS as a part of the reconciliation between the Employer Reserve System and the general ledger. This new process will ensure that benefit payments from RIBS are recorded accurately to the respective general ledger accounts. Fiscal Services will implement this new process as a part of the mid year and annual closing for fiscal year 2007-08.

Self-Funded Healthcare Premiums

Observation #8. Blue Cross is the third-party administrator of the self-funded PERSCare and PerChoice heath plans. Blue Cross reconciles, on a monthly basis, premiums received from the State of California (State), along with the related enrollment records. During our testing of the PERSCare and PERSChoice premiums for the State's active and retired members, we noted the monthly premium reconciliations were not completed in a timely manner and discrepancies were not properly investigated and resolved. The May premium reconciliation was completed in October and the June reconciliation had not been completed as of the end of October. The Blue Cross premium reconciliations identified the following unresolved discrepancies:

- Members were covered under one of the plans, but were not included in participant records provided by the State; therefore, premiums were not paid.
- Members were covered and premiums were paid, but members were not included in participant records provided by the State.
- Blue Cross records indicate members are covered, but CalPERS records do not indicate coverage and members were not included in participant records provided by the State.
- Payments made by the State differ from the established premiums for selected coverage.

We recommend that management establish procedures to ensure Blue Cross enrollment records are reconciled to CalPERS and State data in a timely manner. In addition, we strongly recommend that discrepancies are investigated and resolved prior to the next billing cycle or within a reasonable timeframe.

Observation #8 (Continued)

Management Response:

Health Benefits Branch concurs with the recommendation. The Office of Health Plan Administration (OHPA) and the Office of Employer and Member Health Services (EMHS) will develop processes to ensure that reconciliation reports will be completed timely. OHPA will work with EMHS and the Third Party Administrator (Blue Cross) to investigate and resolve discrepancies in a timely manner

INTERNAL CONTROLS OVER BENEFIT PROCESSING

Retiree Files

Observation #9. In selecting our sample for testing Legislators' Retirement System (LRS) benefit payments, we noted nine instances in which retiree files did not contain the required documentation. Five member files did not contain the appropriate retirement application, and four files did not contain required proof of age or other documentation. In testing internal controls over the Judges' Retirement System (JRS) benefit payment process, we noted four instances in a sample of 40 of retiree files in which retirement applications could not be located and one instance in which the application was incomplete. Retirement applications include the benefit options selected by retirees as well as other key information used in the calculation of benefits. Without complete retiree files, we were unable to determine whether benefit calculations were correct.

In addition, we noted retiree documents for both the LRS and JRS are not imaged in the Document Management System (DMS) in a timely manner, which increases the risk that documents will be misplaced.

We recommend the responsible department create a checklist specifying the forms and documents required for processing retirement applications. To ensure the completeness and accuracy of retiree files, staff processing retirement applications should initial each item on the checklist once the documentation has been verified and placed in the file. Supervisory personnel should independently review all retiree files to ensure documentation is complete and the checklist is signed off. In addition, retiree documents should be imaged in DMS in a timely manner, and there should be a centralized filing system for documents which have not been imaged in DMS.

Observation #9 (Continued)

Management Response

We concur that some documentation is missing but this is primarily in connection with the older LRS files. We are updating our current policies and procedures to require that all LRS retirement files contain an LRS checklist and a new LRS calculation review form. This will ensure that receipt of all required documentation has occurred and will enable us to validate that proper payment has been made to the member and/or beneficiary.

We have revised our policies to require that all judges complete a retirement application form. Staff who process judges' retirement benefits have been notified that all judges must complete the appropriate approved retirement application form for either JRS or JRS II when applying for retirement. If a judge submits a letter in lieu of a retirement application, staff will send a retirement application form to the judge and will not complete the retirement process until the retirement application has been received. In addition, we are making the retirement application available to the judges on our CalPERS website.

Regarding pre-process imaging, since JLVO does not have an automated workflow system, pre-process imaging would not be practical or efficient. As a result, all incoming documents are imaged to DMS on a post-processing basis. It is our understanding that this issue will be resolved with the Pension Resumption System (PSR) project as all core processes, including retirement benefit and health related processes for the CalPERS, Judges' and Legislators' retirement systems will have a workflow system. In the interim, we will establish a new policy requiring staff to forward the documents to DMS within two weeks following completion of the review.

Based on current staffing levels and workflow volumes, it is not feasible for supervisory personnel to review all retiree files. However, we will continue to conduct a detailed post-audit review of member transactions on a routine basis. A separate staff person who is independent from the transaction processing, will conduct the post-audit review of all retiree files, and insure that the existing checklists are completed correctly and that all required documentation has been received.

Manual Calculations

Observation #10. In testing internal controls over the LRS benefit payment process, we observed that LRS pension benefits are manually calculated and input into the Legislators' Monthly Roll System (LEG) subsidiary system by CalPERS staff. Such manual processes are inherently inefficient and prone to error.

We recommend that management consider automating the benefit calculation process.

Management Response:

We agree with this finding and will be automating the benefit calculation process in the Pension System Resumption (PSR) project, and the LEG subsidiary system will be replaced. In the interim, we have developed a calculation review form that will contain all the information used in the calculation of the retirement benefit. Staff preparing the calculation and performing the peer review will initial the document.

General Ledger Posting of Benefit Payments

Observation #11. In testing internal controls over the JRS benefit payment process, we noted two instances in a sample of six months in which the benefit payment claim schedules did not contain the required signature indicating the claim schedule had been reviewed and approved by appropriate supervisory personnel. Fiscal accounting utilizes the claim schedules to record benefit payments in the general ledger system. A signature on the claim schedule indicates that supervisory personnel have reviewed the amounts reported in the claim schedule for accuracy.

We recommend that Fiscal Services ensure the claims schedule has been reviewed and signed prior to posting transactions to the general ledger.

Management Response:

Fiscal Services concurs with the recommendation. Fiscal Services will ensure that claim schedules are signed before posting of the information. Fiscal Services will maintain copies of the reviewed and signed claim schedules as substantiation for transactions posted to the general ledger.

ACCOUNTING FOR OTHER POSTEMPLOYMENT BENEFITS

Observation #12. CalPERS adopted the provisions of Governmental Accounting Standards Board (GASB) Statement No. 43, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans* (OPEB). The implementation of GASB No. 43 required CalPERS to establish two new funds. The California Employers' Retirement Benefit Trust Fund (CERBTF) was established to account for activities relating to the CalPERS prefunded OPEB plan. The Contingency Reserve Fund (CRF) agency fund was established to account for activities that were previously reported in the CRF enterprise fund. We experienced delays in the financial reporting and audit process because CRF agency fund transactions could not be easily extracted from the CalPERS general ledger.

We recommend that management should establish a process to easily identify and record CRF agency fund activities and that management should consider establishing a separate general ledger fund or sub-fund to account for these activities.

Management Response:

FCSD concurs with the recommendation. Fiscal Services will establish a process to easily identify and record CRF agency activity. A new process will be developed which will fulfill the objective of creating records of health premium transactions that are clearly and conveniently organized to facilitate validation and analysis by management and then by independent auditors. This new process will also produce financial statements that comply with the requirements of GASB No. 43. The new process will include transactions beginning with July 2007 and will be completed for the 2007-08 financial statements and audit.

PERF ADMINISTRATIVE EXPENSE BILLINGS

Observation #13. During our testing of administrative expenses, we determined that charges from the Public Employees' Retirement Fund (PERF) to the CRF enterprise fund were not billed in a timely manner. PERF administrative charges for September through December 2006 were not invoiced until February 2007, and charges for February through March 2007 were not invoiced until May 2007. Timely invoicing ensures that revenues and expenses are recorded in the proper period.

We recommend that management should develop and enforce policies to ensure timely billings for administrative charges between CalPERS funds.

Management Response:
Fiscal Services concurs with the recommendation. Fiscal Services will develop policies and procedures to ensure timely billings for administrative charges between CalPERS funds.

GENERAL CONTROLS ELECTRONIC DATA PROCESSING

Information Technology Agency Level Controls

Observation #14. CalPERS policies state that all newly-hired employees will review the CalPERS Information Security Policies and Practices and sign an Information Systems Security and Confidentiality Acknowledgement (ISSACA) form. In addition, all current employees will review and re-sign the form yearly. The form states, among other items, that the employee agrees to abide by CalPERS information systems requirements including the understanding that:

- CalPERS information assets and computer resources only for CalPERS approved purposes.
- Employees are to access CalPERS systems and networks using only my assigned user identifiers and passwords.
- Employees are to notify the CalPERS Information Security Officer immediately of any actual or attempted security violations including unauthorized access; and, theft, destruction, or misuse of systems equipment, software, or data.

While CalPERS policy is that all new-hires complete and sign the ISACCA form and current employees re-sign the form yearly, we found that evidence of the signed forms are not always maintained. Our testing of 18 new-hire forms found that 17 percent could not be found. In addition, we tested six current ITSB employees and were only able to find four completed forms.

The lack of available signed forms could indicate that either the employee did not complete the review and subsequently sign the form, or that the form had been misplaced. In either case, the evidence of completion of the form is not available putting the agency at increased risk for non-compliance to the information security policies and practices.

In addition, CalPERS has performed an IT risk self-assessment documenting the organizational and management practices, personnel practices, data security practices, information integrity practices, software integrity practices, personal computer security practices, network protection practices and incident response practices. These practice areas were rated with an overall risk score derived from a probability, impact and mitigation control assessment score. The documentation was not readily available to support the effectiveness of the mitigating controls noted in the report. It is these mitigation controls that address the vulnerabilities of the agency and which should be assessed for effectiveness.

Observation #14 (Continued)

Recommendations:

1. CalPERS ISO (Information Security Office) should institute new procedures to ensure that training is provided and new-hires sign the ISSACA form. Periodic internal reviews should be accomplished to ensure this is being done. In addition, procedures should be implemented to ensure that recurring training is accomplished and the recurring ISSACA form is signed and submitted to the Human Resources Department.

2. While an IT risk self-assessment has been performed and is an appropriate step in the development of a comprehensive risk assessment strategy for the agency, the ITSB Technology Services and Support Division should consider the documentation and testing of the mitigation controls noted within the current self-assessment. The effectiveness of the mitigation controls should be established and documented in order to substantiate the mitigation control score used within the risk self-assessment.

Management Response:

1. Management concurs with this recommendation. CalPERS Information Security Office (ISOF) has implemented an annual mandatory web-based training (WBT) program that replaces the ISSCA process. This program ensures that all staff, including civil service employees, retired annuitants and student assistants, have been informed, through the WBT, of the CalPERS information security policies and practices, and captures their acknowledgement of and agreement to abide by, the same.

   The WBT process creates a file consisting of the identity and date of everybody who has taken the training. This file is used as a compliance monitoring tool, in lieu of reviewing individual employees' personnel files looking for the most recent Information Systems Security and Confidentiality Acknowledgement (ISSCA) forms.

   The Division Chief of the Information Technology Administration Division (ITAD) has taken the following steps to mitigate issues within the Information Technology Services Branch (ITSB):

   - A notice to all ITSB staff was distributed requesting an Information Systems Security and Confidentiality Acknowledgement (ISSCA) form be reviewed and signed by all employees. ITAD staff is in the process of tracking and monitoring the forms received to ensure all forms are accounted for.

Observation #14 Continued

- All ITAD staff that process badge requests have been made aware and instructed to follow the policy and procedures documented in the ITSB Policy and Procedures Manual which states that a signed ISSCA form must be attached to the Badge Access Card Request form for new ITSB State employees, student assistants, retired annuitants, contractors, and consultants.
- The ITAD staff is aware that each ITSB employee is required to review and sign a form annually as stated in the ISSCA Practice. ITAD staff have developed processes to ensure each employee is instructed to review and sign a form annually as stated in the ISSCA Practice. ITAD staff will also ensure the forms are received and forwarded to Human Resources.
- In addition, ITAD will share this finding and recommendation with the CalPERS Information Security Office to ensure that all recommended actions to resolve this issue are implemented and coordinated as needed.

2. Management concurs with this recommendation. ISOF owns and oversees the CalPERS security risk assessment process. ISOF has implemented RAMP (Risk Assessment and Management Program) to assess, measure, report, recommend remediation, and track implementation of those remediation on a biennial cycle, as defined in the State Administrative Manual (SAM). RAMP consists of three main activities: 1 - structured interviews based on the RiskWatch methodology and tools; 2- document and artifact assessment; and 3- Certification and Accreditation of all new projects prior to implementation. Self-assessments, such as the one that ITSB conducted earlier this year, are not part of RAMP. Self-assessments are a good approach for an organization to take to identify and remediate issues, but do not replace the need for the independent assessment activity represented by RAMP.

Access to Programs and Data

Observation #15. Network password configuration standards are not being enforced. The CalPERS Information Security Office has published a formal Information Security Password Practice policy, last updated in 2005. The policy defines a minimum password length and configuration standard. However, the CalPERS network is currently configured with Novell Network managing file and server access and Microsoft Active Directory managing all other network access. This dual separation of network control has resulted in the inability to electronically enforce a password configuration standard. CalPERS is aware of this inability and is currently in the process of moving all of the network control under Microsoft Active Directory. Until then, though, password configuration standards are not being electronically enforced.

Observation #15 (Continued)

While assignments to the Active Directory Domain, Schema, and Enterprise Administrative Groups are reviewed by the Windows Directory and Network Services (WNDS) manager to ensure that assignments to the groups are limited and appropriate for the employee's duties, there are no formal guidelines or policies defining who should formally have access to these Admins Groups within Active Directory. Without formal policies defining the positions and duties that would necessitate assignment to these sensitive authorization groups, it is left to personal discretion and institutional knowledge which may be subject to inconsistency depending upon who is ultimately authorizing the access.

CalPERS uses an in-house application, Movaris, to manage the workflow used to authorize user account access and authorizations to the various member benefits information systems; CRS, Comet, and RIBS. A review of the process, however, finds that the designated data owners or their formal designees as reported to the Information Security Office, are not required to provide formal authorization prior to a user being allowed access to the application or data. This has the potential to increase the risk associated with the disclosure or integrity of the data as the data owner is not the final approval authority granting access.

Shared accounts are being used by the database administrators when accessing the Oracle database or the VSAM file environment. The use of these shared accounts creates a situation wherein actions taken within the database system cannot be tracked back to a specific individual. Inadvertent or malicious activity may not be able to be positively associated with a specific individual essentially eliminating an effective audit trail.

Database administrator with accounts to the Oracle database or the VSAM environments may potentially have the capability to alter member information affecting benefits payments. Tests have not been conducted to determine if the database systems have sufficient logging triggers or oversight such as file balancing or reconciliations to verify if unauthorized changes can be detected.

Recommendations:

1. Until the CalPERS network environment is consolidated within Microsoft Active Directory, the Information Security Office should periodically run a password cracking application to test the complexity of network passwords. Individuals who are found to have used passwords that do not adhere to the CalPERS Password Practice policy should be notified to update their passwords immediately.

Observation #15 (Continued)

2. The CalPERS WNDS manager should develop and implement formal guidelines or policy defining which positions or duties should be allowed access to the Domain, Schema, or Enterprise Admins Groups within Microsoft Active Directory. This guideline or policy should ensure that only a minimal amount of personnel are allowed access and that the access is critical to the performance of their duties.

3. The CalPERS ITSB should work to ensure that the Movaris application process includes procedures for the formal data owner or the data owner designee to provide approval prior to granting access to an application or data under the responsibility of the data owner. Current user application accounts should also be reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.

4. CalPERS ITSB should evaluate the use of shared accounts and discontinue their use where it has been determined there is a risk to the database. Database administrator accounts with schema owner access should be controlled with access granted sparingly and only after proper approval has been granted.

5. The CalPERS ISO should conduct testing to determine if persons with schema owner access to the Oracle database or to the VSAM files can make changes to the database that would affect member benefits without detection.

Management Response:

1. Management concurs with this recommendation. ISOF published the Identity Authentication Practice in March 2007 to sunset the Password and Shared ID Practices. CalPERS is aware of the inability to electronically enforce all requirements outlined in the Identity Authentication Practice due to the limitations of the technology and dual network control. However, CalPERS does electronically enforce mandatory change periods, password length, password history and system lockout requirements contained in the published practice. ITSB currently has a CalPERS project to migrate the Novell Network to the Microsoft Active Directory environment which will allow for greater password compliance. At the completion of the project the WNDS Unit manager will electronically enforce all of the Identity Authentication Practice requirements where possible.

   ISOF provides awareness training and information regarding the importance of using "strong" passwords. This subject is covered at length in the annual mandatory security awareness training provided to all employees. It has been the subject of several email awareness messages published by the ISOF, the most recent of which was just three months ago. It is also covered in New Employee Orientation.

Observation #15 (Continued)

The ISOF will consider the possibility of implementing random password cracking as a compliance tool, after a thorough analysis is completed. This analysis will include a survey of other state departments' position on the use of password cracking for compliance purposes, best business practices, and industry standards.

2. Management concurs with this recommendation. The CalPERS WNDS Unit manager and Active Directory data owner will develop and implement formal procedures defining access to the defined Administrator Groups within Active Directory in accordance with the existing published Access Control and Data Ownership ISO Policies. This effort will be completed by January 31, 2008.

3. Management concurs with this recommendation. We agree that data owner approval should be obtained prior to granting system access; however, CalPERS Senior Leadership has determined that no modifications will be made to the Movaris application. Movaris will be de-commissioned with the implementation of an Enterprise Identity and Access Management System (EIAM). EIAM will contain the data owner approval functionality.

   Data owner approval is currently obtained for COMET requests through Movaris, but Movaris does not include that same functionality for RIBS and CRS. We are looking into the feasibility of running a monthly report of RIBS and CRS system users for the data owners to review and approve. While this process would be 'after the fact', it is a reasonable mitigation until CalPERS implements its Enterprise Identity Access Management System.

4. Management concurs with this recommendation. To address the shared accounts used to access VSAM files, SAS will review all 'generic' and shared accounts and will work to bring them into compliance with the Identity Authentication Practice (see Observation 1.7 of the internal (FISMA) audit).

   To address shared accounts used to access Oracle databases, a single schema owner account is required by the Oracle DBMS in order to create database objects (e.g. tables, indexes, primary keys). This single owner account owns the database objects. TSSD has an operational need to allow more than one DBA to use the schema owner account and access is granted only when necessary. To mitigate the risk, the ISOF is implementing the Guardium SQL Guard appliance. This appliance provides an audit trail and is outside the control of the DBA's. Logs created by the Guardium will be routinely evaluated by the ISOF to ensure no unauthorized activities, including database schema changes, occur. The testing and implementation of the Guardium should be completed by June 2008.

Observation #15 (Continued)

5. Management concurs with this recommendation. Controls should be in place to ensure modifications to schemas and any other changes to databases are recorded in non-repudiable log files. The ISOF has purchased Guardium SQL event logging appliance to address this issue. During testing of the Guardium appliance, the Information Security Office will verify that Guardium appliance flags unauthorized activities performed by the database administrators (e.g. changing member information in the database that affects benefit payments).

   The ISOF is also verifying VSAM logging processes and will expand its compliance program to include monitoring of event logs in VSAM environment to ensure timely identification of unauthorized database activities. Pending approval of the mid-year FBR, the compliance program will be in place by March 2008.